

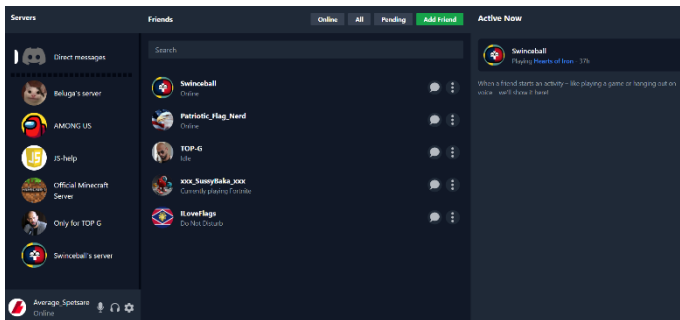
The Real(ly insecure) World

Uppgift för 220s CTF

Simon Meier

Min CTF uppgift är inspirerad av hackningen av Andrew Tate's discord klon "the real world." Här är en rolig video om händelsen: [The Andrew Tate Hack is Worse than you Think... - YouTube](#)

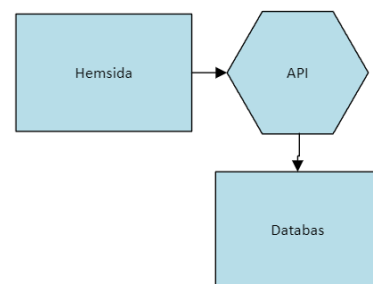
Beskrivning av uppgiften



Jag har byggt en hemsida som har samma utseende som discord. Du är inloggad som en användare (Average_Spetsyare) som redan har varit aktiv och du har några vänner. Målet med uppgiften är att läsa privata chattar mellan dina vänner, där flaggan kommer att finnas.

Hemsidan fungerar rätt så enkelt. All data hämtas med en API från en databas på samma server där api'n körs. Svagheten finns vid API'n.

API'n använder sig av python biblioteket fastAPI. Svagheten ligger vid att man kan enkelt hitta varje användares ID, eftersom svaren på API anropen är publika. Det är med hjälp av båda användarnas ID som adressen till chat historiken skapas. De kombineras enligt den enkla krypteringsmetoden som kan ses på bilden nedan:



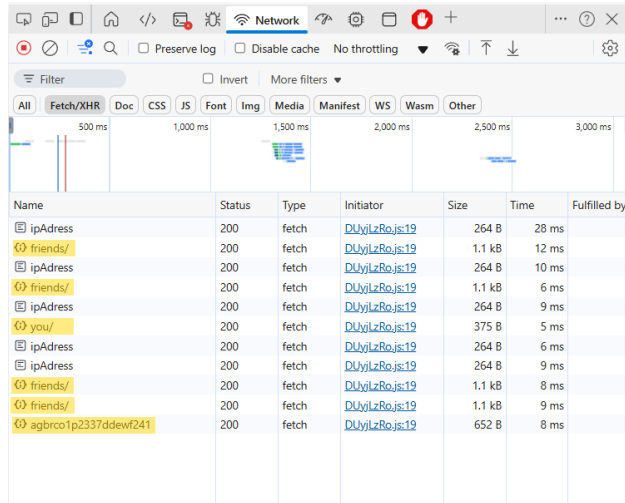
aaaaaa + bbbbbb  abababababab

Genom att hitta detta kan man sedan kryptera sin egna chat ID och läsa andra användares chattar.

Tekniskt, när hemsidan laddar in kommer den att hämta alla användare som du är kompis med. När alla kompisar har hittats kommer ett till API anrop göras där alla chattar med dina kompisar laddas in. Det är dessa API anrop som använder sig av överstående krypteringmetod och som är svagheten. Slutligen har jag använt Nuxt och Tailwind för att designa min hemsida.

För att se hur du kan sätta upp hemsidan på Raspberry PI där API'n och Hemsidan kommer hostas kolla på Github read.me

Detaljerad Lösningsskiss



Name	Status	Type	Initiator	Size	Time	Fulfilled by
ipAddress	200	fetch	DUyilzRojs:19	264 B	28 ms	
friends/	200	fetch	DUyilzRojs:19	1.1 kB	12 ms	
ipAddress	200	fetch	DUyilzRojs:19	264 B	10 ms	
friends/	200	fetch	DUyilzRojs:19	1.1 kB	6 ms	
ipAddress	200	fetch	DUyilzRojs:19	264 B	9 ms	
you/	200	fetch	DUyilzRojs:19	375 B	5 ms	
ipAddress	200	fetch	DUyilzRojs:19	264 B	6 ms	
ipAddress	200	fetch	DUyilzRojs:19	264 B	9 ms	
friends/	200	fetch	DUyilzRojs:19	1.1 kB	8 ms	
friends/	200	fetch	DUyilzRojs:19	1.1 kB	9 ms	
agbrco1p2337ddewf241	200	fetch	DUyilzRojs:19	652 B	8 ms	

Gå runt på hemsidan och kolla sedan i network för att se alla fetches som hemsidan har gjort.

Här kommer man se tre viktiga: friends/, you/ och (string av bokstäver och siffror)/

Genom att kolla svaren på alla kan man se att you/ är information om dig själv, friends/ som är information om alla dina friends och slutligen id:et som är chatten mellan dig och en kompis.

Genom att läsa alla öppna chatar och kolla på alla dina kompisars information kan man komma på att flaggan borde finnas i chatten mellan de två personerna som gillar flaggor. (Patriotic_Flag_Nerd och ILoveFlags).

Genom att examinera alla bokstäver och siffror av chat ID'n kan man se att vartannat tecken alltid är samma på varje ID, och om man slår ihop dessa tecken så blir det id:et på dig själv som man kan hitta i you/.

Genom att fortsätta examinera ID på chatten och ta bort de delar som är en del av ditt id för man fram id:et på den personen som du chattar med. Så då har du kommit på att den enkla krypteringen följer detta mönster

aaaaaa + bbbbbb  abababababab

Du kan då konstruera ditt egna id genom att kombinera ID på Patriotic_Flag_Nerd och ILoveFlags (som du kan hitta i friends/) och genom att sen gå in på

10.22.5.91:8000/chat/xhyizj526374gqhr8s95

eller

10.22.5.91:8000/chat/hxiyiz253647qgrhs859

och läsa vad de har skrivit till varandra så hittar du att de har skrivit den hemliga flaggan till varandra.

Grattis! Du klarade min CTF!!!

Svårighetsgrad

Jag tror att svårighetsgraden ligger runt 0,9. Anledningen är för att det inte är så mycket man måste göra utan man ska bara hitta att svagheten ligger vid API anropen och hitta den enkla krypterings metoden. Jag har det dock inte på 1 eftersom vissa elever kanske inte har jobbat med API på länge (hösten i tvåan) och därför inte ser kopplingen.

Flagga

Den hemliga flaggan är: CTF220s{union_jack}

Reflektion kring skillnader

Den största skillnaden mellan planeringen och utförandet är att jag inte lyckades implementera CORS policy för min API som planerat. Planen var att göra så att man inte skulle kunna nå API:et från browsern utan bara kunna nå det genom hemsidan. Problemet var att jag missuppfattat vad CORS policy gör så den lyckades bara delvis blocka access till API:et, och då bara när man försökte nå det från en egen hemsida men inte om man bara sökte på det i browsern. Därför valde jag att bli av med CORS policy, vilket också gjorde CTF'en enklare och därför ändrade jag till 0,9.

En annan skillnad var hur jag krypterade vägen till chat historiken. Istället för att bara slå ihop användarnas id så krypterade jag de. På ett väldigt simpelt sätt men det gör i alla fall CTF'en lite svårare åt.